8Г

УДК 004.75:004.056:004.272.23

С.Я. Гильгурт, А.К. Гиранова
Институт проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины, г. Киев
hilgurt@ukr.net

Программно-аппаратная защита данных в распределенных интеллектуальных системах

В статье сформулирована актуальная задача расширения возможностей системы безопасности грид-инфраструктуры с целью дополнительной защиты конфиденциальных данных пользователя от несанкционированного доступа со стороны авторизованных пользователей грид-системы, а также от персонала, обслуживающего грид-узлы. Предложено решение на базе реконфигурируемых вычислителей.

Введение

Параллельные вычислительные интеллектуальные системы требуют для своей реализации существенных ресурсов. Распределенные компьютерные среды типа грид [1], получившие широкое распространение в последнее время, представляют собой подходящую техническую базу для таких решений. Данная технология на сегодняшний день, фактически, еще находится в стадии становления. Одной из актуальных проблем здесь остается решение вопросов информационной безопасности.

Тенденция отчуждения (физического и логического отдаления) пользователя от вычислительных ресурсов требует создания новых средств информационной защиты. Как показывает анализ последних публикаций, существующие в современных грид-сетях средства безопасности ориентированы на защиту от внешних по отношению к грид-инфраструктуре субъектов, в то время как вопросы закрытия данных пользователя от авторизованных пользователей системы, а также от персонала, обслуживающего грид-узлы, остаются открытыми.

Дополнительные трудности также возникают при обработке больших объемов информации в связи с тем, что штатные средства информационной безопасности грид-систем (в частности, механизм открытых ключей на базе асимметричных алгоритмов) способны существенно загрузить компьютер пользователя, отправляющего данные на удаленный узел.

Целью данной работы является решение вопросов повышения защищенности конфиденциальных данных пользователей как от внешних, так и от внутренних по отношению к грид-системе злоумышленников, а также ускорения реализации функций безопасности. В качестве технического средства предлагается применение реконфигурируемых унифицированных вычислителей (РУВ) на базе программируемых логических интегральных микросхем (ПЛИС) [2].

Подсистема безопасности грид

Грид можно определить как инфраструктуру, предназначенную для распределенных вычислений, состоящую из отдельных географически разнесенных компьютерных ресурсов: процессоров, оперативной памяти, хранилищ данных.

Инфраструктура грид включает в себя:

– вычислительные ресурсы – отдельные компьютеры, кластеры;

– ресурсы хранения данных – диски и дисковые массивы, системы массового хранения данных;

– скоростные каналы связи;

– специализированное программное обеспечение среднего уровня, так называемое middleware.

Изнутри грид представляет собой многоуровневую структуру взаимодействующих протоколов, сервисов и интерфейсов, определяющих базовые механизмы, посредством которых пользователи устанавливают соединения с грид-системой, совместно используют вычислительные ресурсы для решения различного рода задач. Структура грид-протоколов разделена на уровни (рис. 1), компоненты каждого из которых могут использовать возможности компонентов любого из нижерасположенных уровней [3].

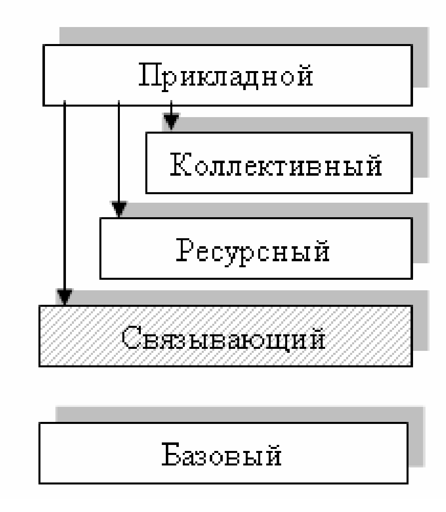


Рисунок 1 – Многоуровневая структура грид-протоколов

Базовый уровень (Fabric Layer) описывает службы, непосредственно работающие с ресурсами.

Уровень связи (Connectivity Layer) определяет коммуникационные протоколы и протоколы безопасности. Коммуникационные протоколы обеспечивают обмен данными между компонентами базового уровня. Протоколы безопасности, основываясь на коммуникационных протоколах, предоставляют криптографические механизмы для идентификации, защиты сообщений, проверки подлинности пользователей и ресурсов.

Ресурсный уровень (Resource Layer) построен над протоколами коммуникации и безопасности уровня связи архитектуры грид. Этот уровень реализует протоколы, обеспечивающие выполнение следующих функций:

– согласование политик безопасности использования ресурса;

– процедура инициации ресурса;

– мониторинг состояния ресурса;

– контроль над ресурсом;

– учет использования ресурса.

Коллективный уровень (Collective Layer) отвечает за глобальную интеграцию различных наборов ресурсов, в отличие от ресурсного уровня, сфокусированного на работе с отдельно взятыми ресурсами.

Прикладной уровень (Application Layer) описывает пользовательские приложения, работающие в среде виртуальной организации. Приложения функционируют, используя сервисы, определенные на нижележащих уровнях.

Рассмотрим подробнее уровень связи.

Для обеспечения информационной защиты в грид-среде используется инфраструктура безопасности грид (Grid Security Infrastructure – GSI). Эта технология обеспечивает безопасную работу в незащищенных сетях общего доступа (Интернет), предоставляя такие сервисы, как аутентификация, конфиденциальность передачи информации и единый вход в грид-систему. Под единым входом подразумевается, что пользователю достаточно один раз пройти процедуру аутентификации, а далее система обеспечивает его автоматическую аутентификацию на всех необходимых ресурсах. Реализация протоколов безопасности выполнена в виде расширения протокола TLS (Transport Layer Security) и основана на криптографических алгоритмах и технологии открытых (публичных) ключей [4]. TLS предоставляет возможность аутентификации и безопасной передачи данных через Интернет с использованием шифрования данных.

В протоколе TLS доступны следующие алгоритмы:

– для обмена ключами и проверки их подлинности применяются комбинации алгоритмов: RSA (асимметричный шифр), Diffie-Hellman (безопасный обмен ключами), DSA (алгоритм цифровой подписи) и алгоритмы технологии Fortezza;

– для симметричного шифрования – RC2, RC4, IDEA, DES, Triple DES или AES;

– для хеш-функций – MD5 или SHA.

В настоящее время в Украине наиболее развитым грид-проектом является Украинский Академический Грид (УАГ), одним из активных участников которого с 2008 года является Институт проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины, где проводится настоящее исследование. На сегодняшний день УАГ, как член сообщества североевропейских государств NorduGrid, в качестве программного обеспечения промежуточного уровня использует платформу ARC (Advanced Resource Connector).

Для выполнения необходимых функций среда NorduGrid поддерживает свои собственные грид-сервисы: Grid Manager, ARC Grid FTP server, SSE, User Interface, Broker, LIS, xRSL, Certification Authority и Grid Monitor.

Постановка проблемы

Процесс выполнения задания пользователя в распределенной вычислительной среде типа грид в общем случае может осуществляться таким образом (рис. 2), что программы, подлежащие выполнению, исходные данные и вычислительные ресурсы, на которых производятся собственно расчеты, расположены на различных грид-узлах.

Для запуска задания в грид-сети пользователь, как правило, использует скрипт-файл на языке xRSL, который содержит все сведения, необходимые для выполнения данного задания, включая информацию о расположении требуемых ресурсов.

Атрибуты inputFiles и outputFiles языка xRSL имеют следующий синтаксис:

(inputFiles=(<имя файла> <расположение>)(<имя файла> <расположение>)…)

(outputFiles=(<имя файла> <расположение>)(<имя файла> <расположение>)…)

Эти атрибуты используются в том числе для управления процессами ввода входной информации на этапе подготовки данных (Preparing), и вывода полученных данных на этапе финализации задачи (Finishing) согласно рис. 3.

Наиболее уязвимой с точки зрения закрытия данных от авторизованных пользователей и от технического персонала грид-узлов информация оказывается во время хранения в виде файлов данных на долговременных носителях информации вычислительных кластеров грид-системы. Поэтому в случае, когда пользователю необходимо обработать в грид-среде конфиденциальную информацию, требуется привлечение дополнительных мер по закрытию данных.

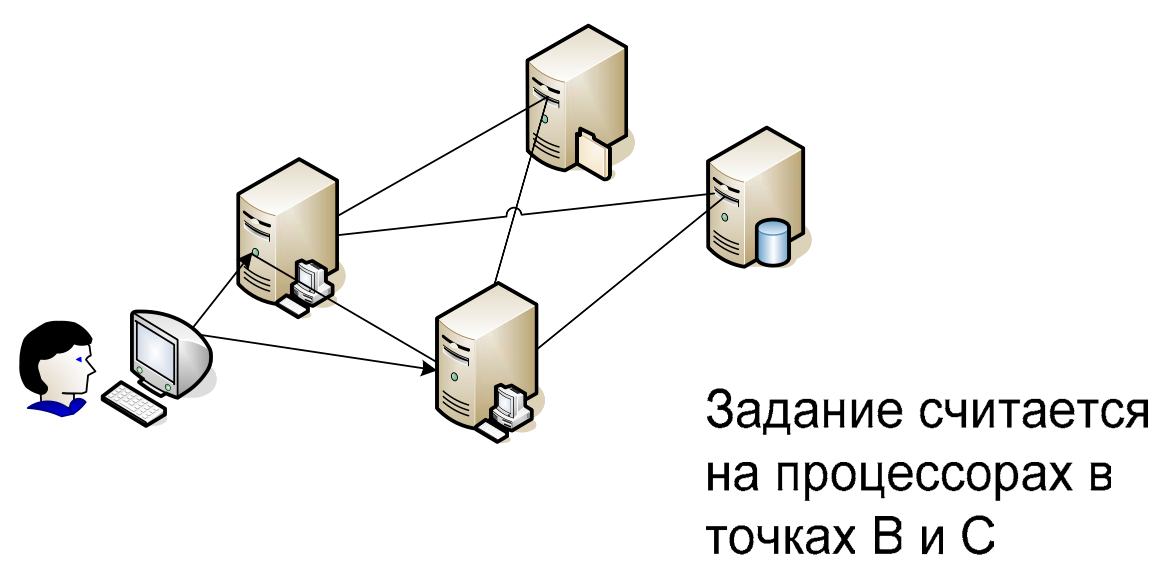


Рисунок 2 – Процесс выполнения задания пользователя в распределенной среде

Самостоятельное применение средств информационной защиты отвлекает пользователя от решения основных задач, требует от него определенной квалификации и не гарантирует достаточного уровня защищенности. К тому же применение только программных средств повышает уязвимость решения и увеличивает время обработки.

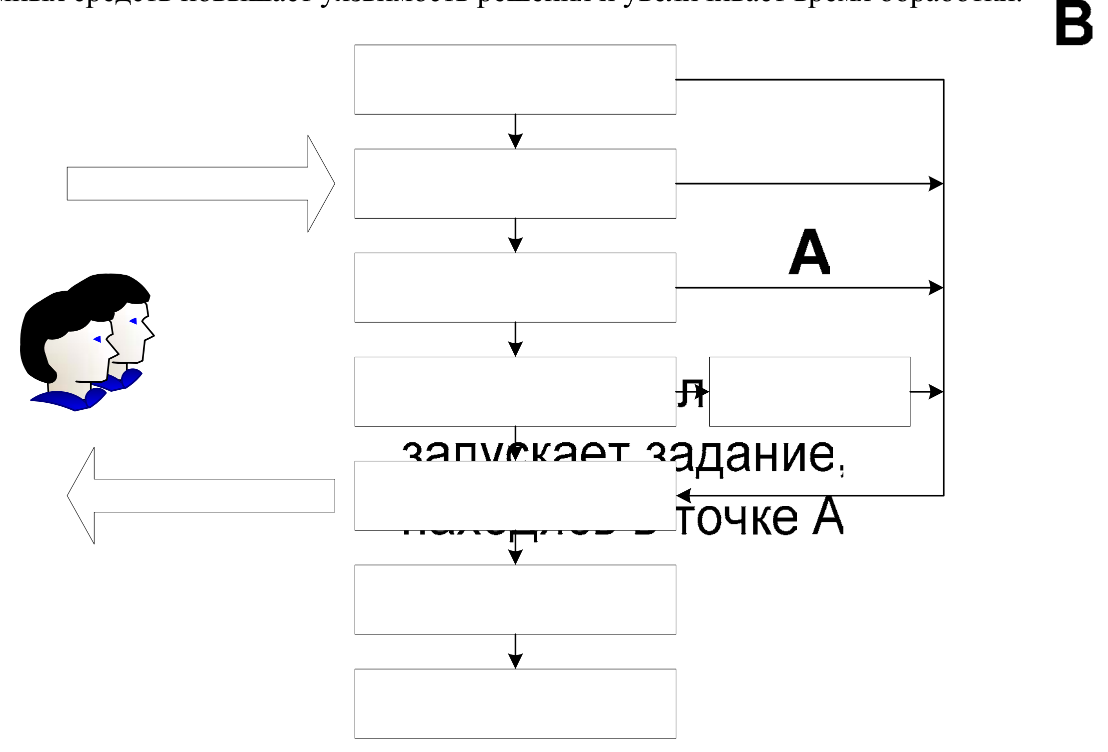


Рисунок 3 – Алгоритм выполнения задания пользователя в грид-среде

Таким образом, актуальной является задача расширения возможностей имеющейся системы информационной безопасности грид-инфраструктуры, в частности, введения дополнительных функций закрытия данных, подлежащих удаленной обработке, а также повышения показателей быстродействия при решении задач закрытия информации в грид-сети.

Задача

Решение на базе реконфигурируемых вычислителей

В настоящей работе предлагается решение, основанное на применении унифицированных реконфигурируемых вычислителей – типовых устройств, построенных на базе ПЛИС. В таком устройстве может быть синтезирована произвольная цифровая схема, например, высокопроизводительный специализированный процессор закрытия информации. Совмещая в себе высокую производительность специализированных вычислений с гибкостью и доступностью универсальных процессоров, РУВ предоставляет возможность эффективного и недорогого решения проблемы, сформулированной выше [2].

Используемые в грид-системе механизмы аутентификации, основанные на применении цифровых сертификатов, позволяют без существенных изменений принципов функционирования грид-среды реализовать на РУВ как стандартные алгоритмы шифрования, так и усиленные методы защиты информации [5].

Механизм реализации вышесформулированных требований к дополнительным функциям подсистемы защиты информации грид-сети выглядит следующим образом (рис. 4).

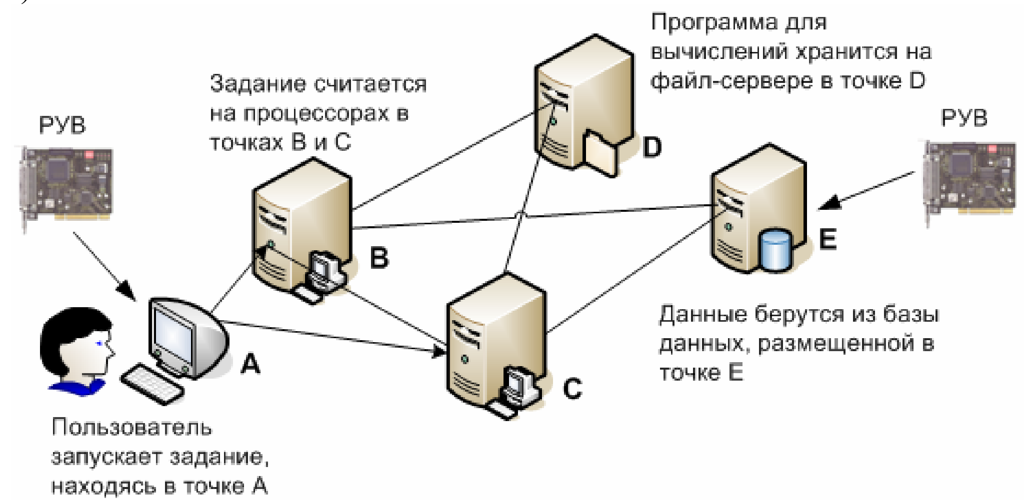


Рисунок 4 – Подсистема защиты информации на базе РУВ

Перед запуском задания на исполнение в РУВ на компьютере пользователя загружается структура специализированного процессора, реализующего требуемые алгоритмы закрытия информации. Данные, подлежащие обработке, после аппаратного преобразования на РУВ (центральный процессор компьютера пользователя при этом практически не нагружается) передаются по коммуникационным каналам на целевой грид-узел и хранятся там в закрытом виде.

Процедура обратного преобразования данных инициируется задачей пользователя непосредственно перед ее выполнением и осуществляется либо с помощью РУВ, установленного на целевом грид-узле, либо программным способом, с использованием вычислительных ресурсов кластера.

В зависимости от того, насколько полно задействуются штатные возможности системы безопасности грид-сети, рассмотренный выше механизм закрытия данных пользователя может быть реализован в нескольких вариантах:

– «прозрачный» режим – максимальное использование штатных средств безопасности грид-инфраструктуры; в этом случае на ПЛИС реализуются стандартные алгоритмы защиты;

– «прозрачный расширенный» режим – с возможностью загрузки в ПЛИС нестандартных, в том числе усиленных, алгоритмов закрытия информации;

– «полупрозрачный» режим, при котором система безопасности грид-инфраструктуры используется только для авторизации и доставки ключевой информации, а процедуры собственно закрытия информации реализуются компонентами программно-аппаратной подсистемы защиты данных при непосредственном участии пользователя.

В каждом из вышеперечисленных вариантов, как на компьютере пользователя, так и на удаленном грид-узле, вместо РУВ возможно использование только программной реализации.

Выводы

Подсистема защиты информации, построенная на основе предложенных подходов, позволяет пользователям грид-сети повысить степень защищенности своих конфиденциальных данных, как пересылаемых в грид-среде, так и хранящихся на удаленных серверах, а также ускорить процесс преобразования больших объемов информации с целью ее закрытия.

Литература

1. Воеводин В.В. Параллельные вычисления / В.В. Воеводин, Вл.В. Воеводин. – СПб. : БХВ-Петербург, 2002. – 608 с.
2. Гильгурт С.Я. О применении реконфигурируемых унифицированных вычислителей для решения научно-технических задач / С.Я. Гильгурт // Параллельные вычислительные технологии (ПаВТ'2008) : труды международной научной конференции (Санкт-Петербург, 28 января – 1 февраля 2008 г.). – Челябинск : Изд. ЮУрГУ, 2008. – С. 358-363.
3. Кирьянов А.К. Введение в технологию Грид : учебное пособие / А.К. Кирьянов, Ю.Ф. Рябов. – Гатчина : ПИЯФ РАН, 2006. – 39 с.
4. Dierks T. The Transport Layer Security (TLS) Protocol Version 1.1, RFC 4346 / T. Dierks and E. Rescorla.
5. Гиранова А.К. Анализ подходов к повышению эффективности закрытия информации и вопросы их реализации на унифицированных вычислителях / А.К. Гиранова // Зб. наук. праць ІПМЕ НАН України. – Київ, 2009. – Вип. 52. – С. 78-83.

С.Я. Гільгурт, А.К. Гіранова

Програмно-апаратний захист даних у розподілених інтелектуальних системах

У статті сформульована актуальна задача розширення можливостей системи безпеки грід-інфраструктури з метою додаткового захисту конфіденційних даних користувача від несанкціонованого доступу з боку авторизованих користувачів грід-системи, а також від персоналу, що обслуговує грід-вузли. Запропоноване рішення на базі реконфігурованих обчислювачів.

S.Ya. Hilgurt, A.K. Giranova

Hardware-Software Data Security Means in the Distributed Intelligence Systems

An actual task of the Grid security system enhancement is raised: user's private data to be protected against another authorized users of the Grid-system including nodes personnel. A solution based on reconfigurable accelerators is proposed.

Статья поступила в редакцию 05.07.2010.